anand guru

SOC EXPERTS

Interview Questions on
IBM QRadar

Anand Guru

Security+ | CySA+ | CEH | ECIH

Founder

SOC Experts

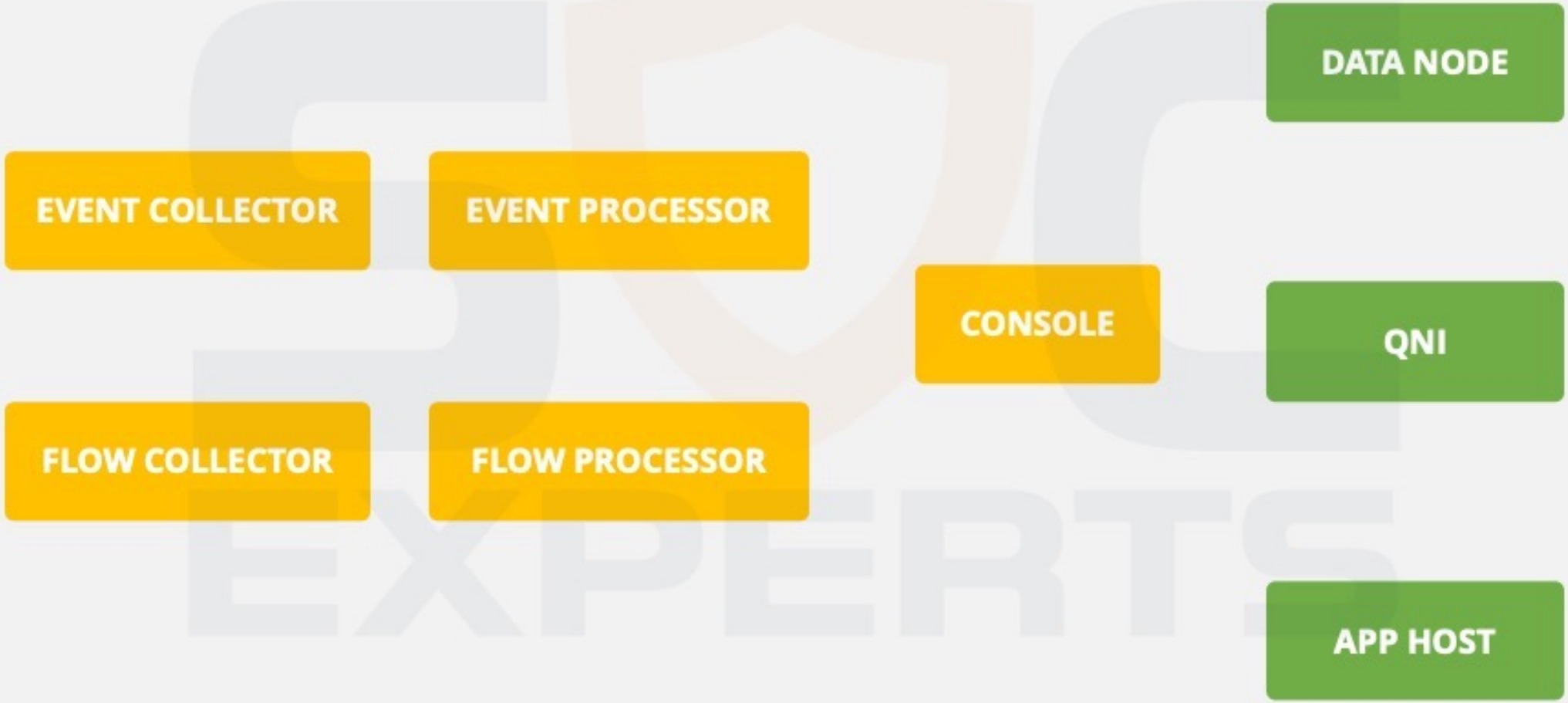
https://socexperts.com

anand guru

Complete IBM QRadar Training

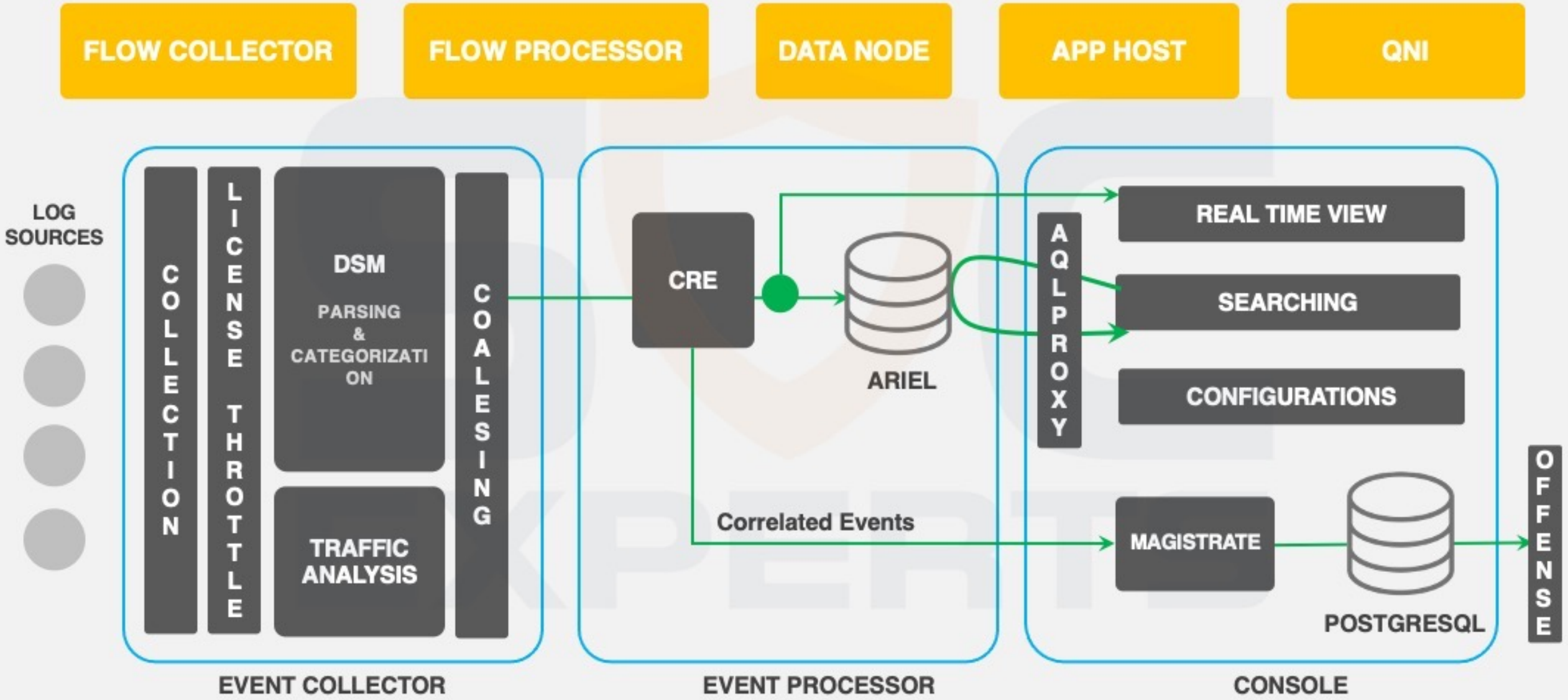
- https://www.securitylearningacademy.com/course/view.php?id=4233
- **IBM QRadar SIEM Foundation Badge**

What are the components of IBM QRadar SIEM?



anand guru

Explain the Architecture of IBM QRadar.



What is Magistrate?

Magistrate is a component that runs on the QRadar Console. It does the following functions:

- **Offense Rules -** Monitors and acts on offenses, such as generating email notifications.
- **Offense Management** - Updates active offenses, changes statuses of offenses, and provides user access to offense information from the Offenses tab.
- **Offense Storage** - Writes offense data to a Postgres database.

EXPERTS

What databases does IBM QRadar use?

- QRadar uses **Ariel database** for storing events. It is a proprietary database of IBM.
- Ariel database sits in Event Processor

  Ariel is flat file structure database. It indexes information based on Time.
- The location of the database are

  `/store/ariel/events` for Events

  `/store/ariel/flows` for Flows
- The language used to query the database is **AQL** (Ariel Query Language)

- QRadar also uses **POSTGRESQL** database for storing asset information and offense data.
- POSTGRESQL is hosted in Console.

anand guru

How does licensing work in IBM Qradar?

For events, QRadar Licensing is done based on **EPS** (Events Per Second)

IBM sells license in multiples of 2500. i.e. you can take EPS of 2500 or 5000 or 7500 and so on.

For flows, QRadar Licensing is done based on **FPM** (Flows Per Minute)

EXPERTS

anand guru

What happens if Event Collector exceeds the license limit?

License Throttle checks if the number of logs coming in at a given second are well within the license limit or not.

If the no. of logs exceed the license limit, the excess logs are parked aside in a buffer. This buffer is of 5 GB.

In the next second, these parked logs in the buffer will be picked up and processed.

E.g.:

Lets assume we have a license of 5000 EPS.

At one point if there are 6500 logs for a second, the excess 1500 events will be parked aside.

In the next second, lets assume 2000 new events come.

1500 parked events + 2000 new events = 3500 events; which is within the license limit and hence they will be processed.

anand guru

Why is this 5GB buffer given?

The buffer is to handle accidental spike in log volumes.

For example when a company is under DOS attack, the number of logs are expected to go high (temporarily till the attack is remediated).

Here the customer need not buy additional license as it is only a temporary condition

EXPERTS

What version of QRadar have you worked on?

The latest version of IBM QRadar is 7.4.0 (7.4.0.20200304)

I started working on QRadar since version 7.2.8 patch 3 (was release on Jan 2017)

SOC EXPERTS

What Protocol Configuration methods have you used in QRadar?

Protocol Configuration are Collection Methods.

The frequently used protocol configurations are :

- **WinCollect**
- **Syslog**
- **Logfile**
- **JDBC/ODBC**
- **API**

SOC EXPERTS

What are the Tabs you see in IBM QRadar

The tabs are:

Dashboard

Offenses

Log Activity

Network Activity

Assets

Reports

Admin

Vulnerability Management (If we have the license)

SOC EXPERTS

anand guru

Name few commonly used Properties (Parameters/Fields)

Most commonly used fields in IBM QRadar are:

Log Source

Log Source Group

Category

Source IP

Destination IP

Destination Port

Username

Source Geolocation

Destination Geolocation

SOC EXPERTS

anand guru

What is Quick Filter?

- The Quick Filter is a search bar that is displayed on both the Log Activity and Network Activity tab in QRadar.
- The Quick filter works similar to a 'Google-style' search where you can add in one or more terms, or use regular expressions.
- Quick Filter queries are run on **Payload (raw logs)** and not meta-data.
- If the quick filter is used in conjunction with other search parameters, the quick filter will execute first, and the remaining search parameters will be used to further filter the results.

E.g.:

socexperts

"soc experts" OR socexperts

/*soc*/

logon AND failure

anand guru

What IBM QRadar Apps have you used?

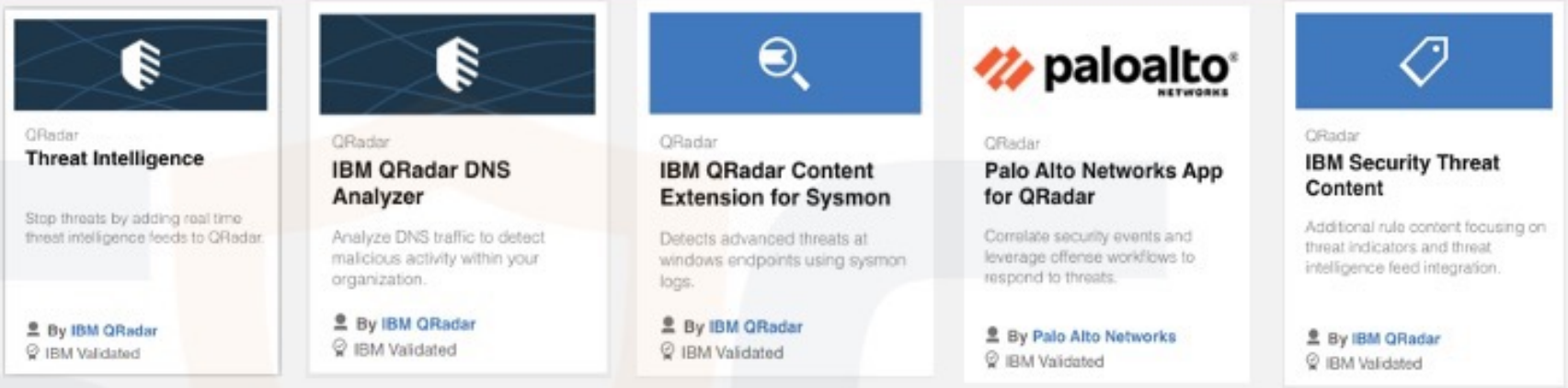
Threat Intelligence

DNS Analyzer

Content Extension for Sysmon

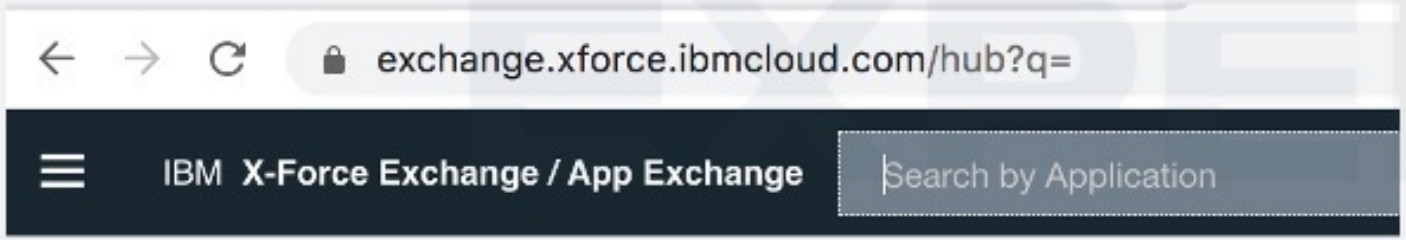
Palo Alto Networks

IBM Security Threat Content


QRadar
Threat Intelligence
Stop threats by adding real time threat intelligence feeds to QRadar.
By IBM QRadar
IBM Validated
QRadar
IBM QRadar DNS Analyzer
Analyze DNS traffic to detect malicious activity within your organization.
By IBM QRadar
IBM Validated
QRadar
IBM QRadar Content Extension for Sysmon
Detects advanced threats at windows endpoints using sysmon logs.
By IBM QRadar
IBM Validated
paloalto NETWORKS
QRadar
Palo Alto Networks App for QRadar
Correlate security events and leverage offense workflows to respond to threats.
By Palo Alto Networks
IBM Validated
QRadar
IBM Security Threat Content
Additional rule content focusing on threat indicators and threat intelligence feed integration.
By IBM QRadar
IBM Validated

From where do you download IBM QRadar Apps?

From **IBM App Exchange**



Explain Rules and Building Blocks in IBM QRadar.

- Also referred as Correlation Rules
- Rules are set of condition that indicate suspicious activity.
- Rules perform tests on events, flows, or offenses.
- If all the conditions of a test are met, the rule generates a response.

- Building blocks are same as rules, but have no actions associated with them.
- Test groups of IP addresses, privileged user names, or collections of event names.
- Building Blocks are used in Rules.

NOTE: Both Rules and Building Blocks are configured at **Offenses (Tab) → Rules**

anand guru

What is Network Hierarchy?

Network Hierarchy is the logical segmentation of network.

The segmentation can be done based on the geolocations or business units or subnet type

Example,

- 10.10.0.0/16 – Corporate Network
- 10.10.5.0/24 – Server Subnet
- 10.12.0.0/16 – Guest Network
- 17.16.0.0/16 – Singapore Office

The purpose of the hierarchy is to help you quickly identify where an offense is happening

Network objects can be used in filters, rules etc.

anand guru

What are Reference Sets?

It is a list of specific type of data.

IOC	**- IP Address**
List of DNS Servers	**- IP Address**
List of Privileged Accounts	**- Username**
List of Countries of Concern	**- Geolocation**

Reference sets can be used in searches, filters, rule test conditions, and rule responses.

EXPERTS

What are retention buckets?

- Retention buckets define how long event and flow data is retained in IBM QRadar.
- The **default retention period is 30 days**; then, the data is immediately deleted.
- You can configure up to **10 retention buckets** for shared data, and up to 10 retention buckets for each tenant.

EXPERTS

Explain Tenant Management in IBM QRadar.

Multitenant environments allow MSSPs and multi-divisional organizations to provide security services to multiple client organizations from a single, shared IBM QRadar deployment.

To create a new Tenant, we must first create a new Domain.

Domains are created based on the log source or collector.

E.g.: As a MSSP we might have placed one Event Collector (**CLIENT-A-EC**) at one of our location, client A. So while creating a domain, we can say all the logs coming from CLIENT-A-EC will be tagged as belonging to one Domain.

Domains help in handling **over-lapping IP addresses**. Example - 10.10.5.4 can be a email server for Client A and the same IP can be a Firewall for Client B

The configuration can be accessed from

Admin tab → Domain Management &

Admin Tab → Tenant Management

anand guru

Can we forward events from IBM QRadar to some other syslog server?

Yes, we can forward logs from QRadar to another server.

We should first configure Destinations Server @ **Admin Tab → Forwarding Destinations**

Then we need to configure a Routing Rule to forward required logs to the Forwarding Destination. This can be done @ **Admin Tab → Routing Rules**

EXPERTS

Can we forward events from IBM QRadar to some other syslog server?

Yes, we can forward logs from QRadar to another server.

We should first configure Destinations Server @ **Admin Tab → Forwarding Destinations**

Then we need to configure a Routing Rule to forward required logs to the Forwarding Destination. This can be done @ **Admin Tab → Routing Rules**

EXPERTS

What kind of back-ups can be taken in IBM QRadar?

The backup archive includes **configuration** information, **data**, or both from the previous day. The size of backup will depend on the amount of event data from that day.

Configuration backups include the following components:
Assets
Custom logos
Custom rules
Device Support Modules (DSMs)
Flow sources
License key information
Log sources
Offenses
User and user roles information

Data backups include the following information:
Audit log information
Event data
Flow data
Report data
Indexes

Default Backup Location - **/store/backup/** directory (It is recommended to change it to a remote server)

Default Backup Frequency – **Everyday midnight**

anand guru

Explain IBM QRadar updates.

The Auto Update pulls 4 types of update

Configuration Updates – Configuration files, QIDMap etc.

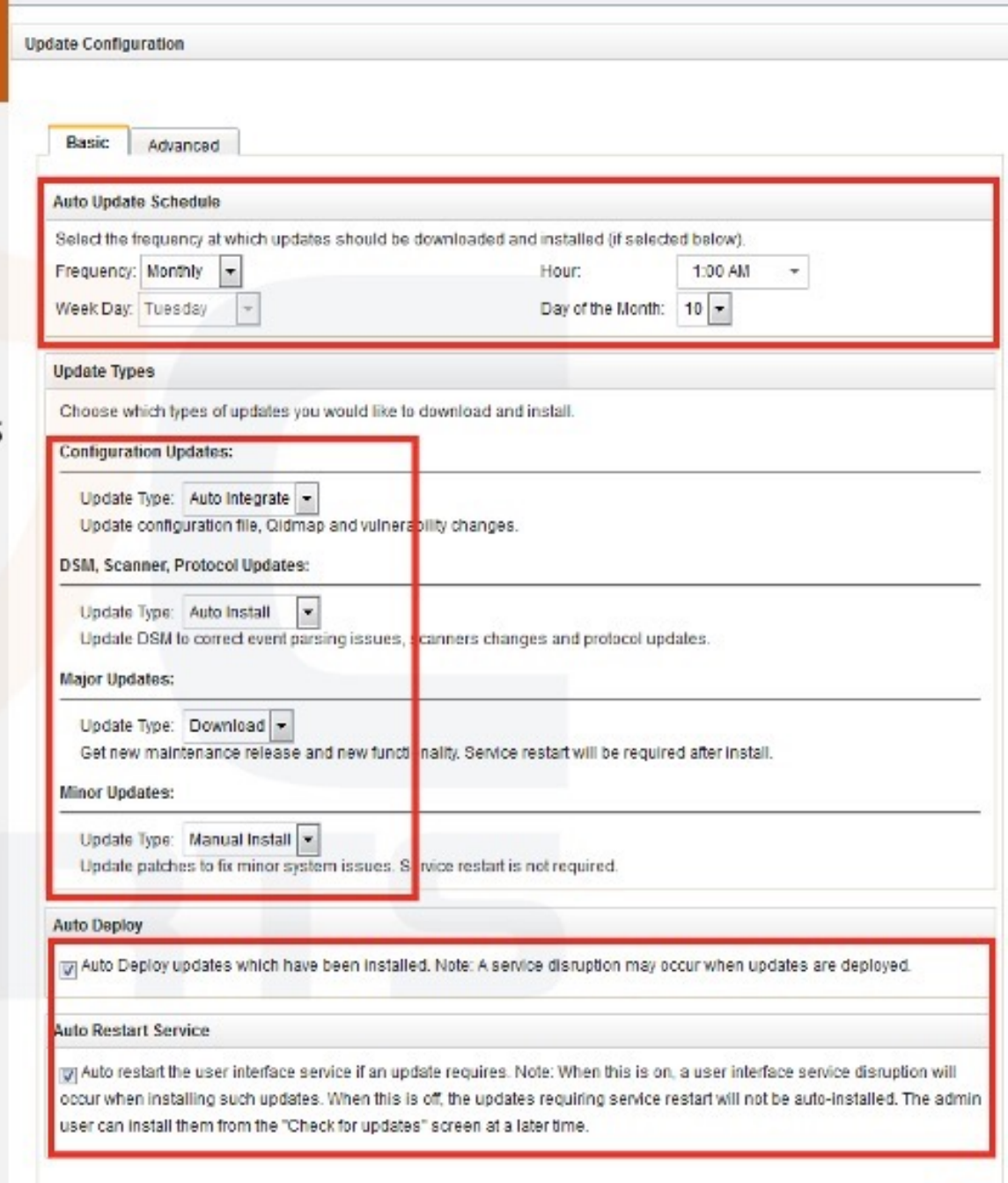
DSM, Scanner, Protocol Updates – DSM, parsers collection methods

Major Updates – Maintenance Releases, new features

Minor Updates - Patches

IBM QRadar Update server - http://qmmunity.q1labs.com

Default update frequency is - *Daily*


Update Configuration
Basic
Advanced
Auto Update Schedule
Select the frequency at which updates should be downloaded and installed (if selected below).
Frequency: Monthly
Hour: 1:00 AM
Week Day: Tuesday
Day of the Month: 10
Update Types
Choose which types of updates you would like to download and install.
Configuration Updates:
Update Type: Auto Integrate
Update configuration file, Qidmap and vulnerability changes.
DSM, Scanner, Protocol Updates:
Update Type: Auto Install
Update DSM to correct event parsing issues, scanners changes and protocol updates.
Major Updates:
Update Type: Download
Get new maintenance release and new functionality. Service restart will be required after install.
Minor Updates:
Update Type: Manual Install
Update patches to fix minor system issues. Service restart is not required.
Auto Deploy
Auto Deploy updates which have been installed. Note: A service disruption may occur when updates are deployed.
Auto Restart Service
Auto restart the user interface service if an update requires. Note: When this is on, a user interface service disruption will occur when installing such updates. When this is off, the updates requiring service restart will not be auto-installed. The admin user can install them from the "Check for updates" screen at a later time.

What are the core services in IBM QRadar?

There core services in IBM QRadar are:

hostcontext	It is kind of master services, that controls most of other services and processes. Monitors all QRadar components to ensure that each component is operating as expected
tomcat	Responsible for loading Web UI and UI interactions.
hostservices	It keeps track of 2 other running processes, Message Queues (IMQ), which opens up communication ports between QRadar Components and PostgreSQL.
ecs-ec-ingress	Event Correlation Service - Event Collector Ingress: collects the events in a buffer while ecs-ec and ecs-ep are being restarted. Then it spools the data back to ecs-ec and ecs-ep
ecs-ec	Event Correlation Service - Event Collector: parse, normalize and coalesce the events.
ecs-ep	Event Correlation Service - Event Processor: correlates events (Custom Rule Engine), stores events in the Ariel database and forwards events matching rules within CRE to the Magistrate component.

anand guru

Frequently used troubleshooting commands

- Command for health check: **drq**

- Check if logs are hitting the collector interface:

  tcpdump –vvnni <interface_name> host <log_source_IP>

  tcpdump –vvnni ens192 host 10.10.50.3

- Check disk space: **df – h**

- Restart a service: **systemctl <command> <service_name>** (Where **command** can be **stop, start, restart, status)**

  systemctl stop hostservices

anand guru